INTERROGATION OF AMTSRAT DR. STIEHLER OF OKM/4 SKL II

ON GERMAN METEOROLOGICAL CYPHERS.

This interrogation was carried out on 23rd June 1945, by Lt.Cdr. Forster, R.N.V.R., in the back parlour of a farm-house at Bargen in the German-controlled concentration area 'G'. The interrogator had little time at his disposal and had no special knowledge of German meteorological cyphers; moreover, circumstances were generally unfavourable for detailed interrogation. He therefore restricted himself to obtaining answers to the questionnaire drawn up by G.C.C.S. It will be seen that answers were not obtained to all the questions.

It was made clear to Dr. Stiehler that though the interrogator had neither the desire nor the power to extract any information from him which he was unwilling to give, Kapitaen zur See LUCAN, the Director of 4 SKL II, had already seen fit to give us such information as he possessed and it was expected that Dr. Stiehler would do the same. He said he was prepared to answer questions. The atmosphere throughout was very tense. Dr. Stiehler apparently expected to be shot or otherwise ill-treated by the interrogator, who was accompanied by another armed officer, but gave away as little as possible.

TICOM
5 July 1945

Copy No. 16
No. of Pages 5

Distribution:

British
1. Director
2. D.D.3.
3. D.D.4.
4. D.D.(N.S.)
5. D.D.(M.W.)
6. D.D.(A.S.)
7-8. A.D.(C.C.R.) (2)
9. Lt.Col. Leathem

TICOM
10. Chairman
11-12. S.A.C. (2)
13. Cdr. Bacon
14. Cdr. Mackenzie
15. Cdr. Tandy
16. Lt.Col. Johnson
17. Lt.Cdr. Manson
18. Major Seaman
19. Lieut. Eachus
20. Lieut. Vance
21. Captain Cowan
22. Lieut. Fehl
23-24. TICOM Files (2)

U.S.
25-26. OP-20-G (2) (via Lt. Pendergrass)
27. G-2 (via Lt.Col. Hilles)
28-29. S.S.A. (2) (via Major Seaman)
30-31. Director, S.I.D. ETOUSA (2) (via Lt.Col. Johnson)

Additional
32. Dr. McVittie
33. Lt.Cdr. Forster

[Note: All the questions were phrased as if we knew nothing more about these cyphers than can be obtained from captured documents which have so far come to hand. The German names, code words, etc., all occur in these documents. In the "Notes to Interrogator" (NTI) are given some further details obtained from cryptanalytic work.]

A. The "Geheimer Wetter- und Seeschluessel der Kriegsmarine"

[NTI: This is the German Naval Met. cypher which used the principle of trigram (3-figure) substitution. It is known from Z sources to have also been called "Marine Wettertauschtafeln".]

1. Q When was this cypher first introduced?

   A 1940.

2. Q What authority was responsible for devising the cypher? Was it adopted as a result of cryptographic tests and, if so, what were these tests?

   A The cypher was devised by Reg.Rat.Dr. RUH of M.W.D. Tests [unspecified] were carried out.

3. Q Were the Tauschtafeln constructed by a machine or by drawing numbers out of a hat? Was any system used in constructing any of them?

   A Dr. STIEHLER devised systems of compiling Tauschtafeln, one consisting of three strips bearing figures in hatted order. These strips were then slid one against the other and the trigrams read off. In approximately 1942 they went over to Hollerith.

4. Q Why are the Tauschtafeln and their reciprocals bound in separate books and not in the same book as with the Luftwaffe Tauschtafeln?

   A It was easier to work that way. Certain ships and stations only needed the encode, others only the decode. Considerable saving of paper was effected by bringing the encode and decode parts out separately.

   [G.C.C.S.Comment: Every so-called "decode" table was in fact also used as an "encode" in some encyphering period or other. The cypher could not have been used by anyone unless both encode and decode books were at hand.]

5. Q What is the significance of the Ausgabe (10th to 20th) mentioned in a Cap.Doc.? Are these all there were and when were they in use?

   A There were up to 22 Ausgaben.

6. Q Was each Tauschtafel used once or more often? Did a complete Ausgabe recur? If so, what was the system of repetition?

[NTI: The answer to both these questions is "Yes", but we want to know what prompted the Germans to commit so stupid a crypto error.]

A Yes. The system was that tables which had been used by central stations, OKM Wewa etc., were later issued to outstations, e.g. in Greece and Italy. The authorities were aware that this was a cryptographic risk, but it was forced on them by the necessity for economy of material.

[G.C.C.S.Comment: the answer is correct as referring to Ausgaben but not as referring to the Tauschtafeln themselves.]

7. Q What is the significance of the 4th, 5th, 7th, 8th, and 9th Sonderausgabe mentioned in the Cap.Doc.? Were these all, when were they used, and for what purpose? How many Tauschtafeln did each contain?

A Sonderausgaben were for emergency use. They were also used by raiders as a standby so that on arrival in European waters traffic could be put out for them specially in a key they could read.

8. Q The Cap.Doc. calls the following "Wichtige Meldungen": reports from U-Boats, from Zenit aircraft, and from "WF-Geraeten" (automatic weather reporters). Were any special precautions taken in encyphering and in distributing these reports?

[NTI: We believe that double encyphering with a table of Sonderausgabe followed by an ordinary Ausgabe table was used.]

A It was considered desirable to restrict the distribution of these reports. They were encyphered with tables known as 'Ysoptafel' and 'Zettafel'.

9. Q The Cap.Doc. mentions SYNOP NACHTIGALL. What were these?

[NTI: Press the victim hard on this point, as these reports have been a mystery throughout the war. They may be decodes of Russian or British cyphers.]

A 'Synop Nachtigall' consisted of decodes of Turkish cyphers. They were not very difficult to read.

B. <u>The "Wettertauschtafeln der Luftwaffe"</u>

[NTI: The G.A.F. Met. cypher : trigram substitution again.]

1. Q Repeat Questions 1, 2, 3, of A again.

A The cypher was devised by Reg.Rat.Dr. WUSTHOFF

2. Q Why was a different cypher needed? Would not one have served both Luftwaffe and Kriegsmarine?

[NTI: The existence of these two cyphers repeating the same texts was another major crypto error made by the enemy.]

A A different cypher was introduced for the Navy because (1) it was found that Naval requirements were different from G.A.F. requirements; and (2) it was thought advisable from considerations of security not to overload the G.A.F. system unduly.

[Note by Interrogator: this point was pressed, but Dr. STIEHLER stuck to it.]

3. Q One captured set of tables shows there were 18 tables (9 reciprocal pairs) to a Heft all firmly bound, another shows a Heft bound in 5 books with 15 reciprocal pairs to a book, the books labelled Gruppe A - E and arranged so that tables can be torn out at a perforation. Why was this change brought in? Was it a security measure?

[NTI: In the earlier type of book each Tauschtafel could be used more than once, in the second it lasted for one period of 24 hours only.]

A Yes, it was a security measure, so that individual tables could be taken in an aircraft without the whole set being compromised in the event of the loss of the aircraft. The state of the book described in the question was transitional only, in order to adapt existing stock to new requirements. Eventually separate tables were brought out.

[Note by Interrogator: Interrogator was unable to get down the whole of this answer to this question.]

[G.C.C.S.Comment: Wettertauschtafeln were never found in German aircraft. Dr. STIEHLER is apparently thinking of air-to-ground or Zenit cyphers.]

4. Q What is the meaning of the code words Temp, Terra, Werot, Zenit found in the Cap.Doc.?

[NTI: The only mysterious one is Werot.]

A 'Werot' stands for 'Wetter Rot'; it corresponds to the Naval 'Sonderwettermeldungen'.

C. <u>The "Sonder-Wettertauschtafeln der Luftwaffe"</u>

1. Q Repeat Questions 1, 2, 3 of A.

A [not asked]

2. Q What was the purpose of having still a third Tauschtafel cypher?

3. Q What were the contents of broadcasts using the cypher?

[NTI: The existence of this cypher may have been due to (a) fear of compromise on the Russian front; (b) lack of faith in Germany's Eastern Allies. It was used in Rumania, Finland and occupied Russia.]

A The cypher was used for reports of a high degree of secrecy.

General Questions on A, B, C.

1. Q Were any Tauschtafeln common to A, B, C?

[NTI: Some common to B and C have been found but, as we recovered C spasmodically, not much is known about this.]

A The 'Sondertafel fuer Atlantikfestungen' was common to all three services.

[Note by Interrogator: Question apparently misunderstood.]

2. Q Were there any more Tauschtafel cyphers?

[NTI: I believe a separate one may have been used for re-broadcasting decodes of Russian Met. cyphers.]

A There was 'Schluessel Schwarzmeer', so called because it was first used in the Black Sea. It consisted of bigram substitution tables and ran from 1942 - 1944.

[Note by Interrogator: No indication that it was used for re-broadcasting decodes.]

D.

1. Q Did the G.A.F. or the German Navy use any other types of cypher system for Met than the Tauschtafeln? If so, what were they and what were they called?

[NTI: We know they used additives, simple-substitutions etc.]

A From 1944 onwards additive one-time pads were used on the British model.

[Note by Interrogator: Dr. STIEHLER showed that he had some knowledge of British Met. systems and evidently expected a series of pressing questions on this point. Interrogator felt, however, that the matter had better not be raised without special briefing and stuck to the questionnaire.]

[G.C.C.S.Comment: Only one small line of one-time

2. Q Why were special codes - rather than the International Met. Code - used for Zenit (Aircraft) observations and those from Polar stations? Who devised these codes?

A The Copenhagen 'Obs' presupposes participation of a large number of widely distributed stations in order to produce a workable synoptic chart. In war-time this is impracticable. It was therefore necessary to devise a code which should reckon with factors not included in the Copenhagen 'Obs'. The latter for instance was particularly weak on 'general nature of the weather'. The person who devised the codes was Dr. STIEHLER himself.

E.

1. Q Who devised and controlled the Met. cyphers used by the Finns, Rumanians, Italians, etc. whilst they were Germany's Allies? Why were additives used and what security measures for controlling the loads were taken? What were they called by the Germans?

[NTI: Italian cyphers were captured; the rest are known from crypto work only.]

A Not known. Ask the Luftwaffe.

2. Q Whose idea was the transposition used for interchange of information between the Russian and German Met. services in 1940-41?

A Not known. Dr. STIEHLER did not join 4 SKL II until the end of 1941.

F

Q Why was it necessary to have so many collective weather broadcasts? Would not one or two have served? Was no distribution of observations made by teleprinter broadcast and, if so, why were W/T transmissions necessary at all?

A Not known. Ask the Luftwaffe. In general the T/P network was unsatisfactory and the elapsed time was very long.